Algorithm to Detect and Recover Wormhole Attack in MANETs

Darshana Sorathiya
PG Scholar Computer Engineering
RK University
Rajkot, Gujarat, India

Haresh Rathod
Assistant Professor Computer Engineering
RK University
Rajkot, Gujarat, India

ABSTRACT

A Mobile Ad-Hoc Network (MANET) is a network in which the mobile nodes are randomly connected with each other. Nodes are dynamically in nature. It usually works by broadcasting the information. Its nature is broadcasting so there is a chance to disrupt network by attacker. The number of attack can be done in Mobile Ad Hoc Network. In this paper we have studied about wormhole attack in AODV. We have analyzed different technique to detect and prevent wormhole attack. In our proposed solution detect and overcome the effect of wormhole attack in MANET.

Keywords

MANET, Wormhole attack, Wormhole detection techniques

1. INTRODUCTION

MANETs is a collection of dynamic mobile nodes. It is a structure less network in which mobile nodes are free to move in any direction. There is no any centralized controller in network. A communication have been established which each other using a multi hop links. It behaves like a router. There is no any base station. It is useful in situations where we have lack of fixed network infrastructure, such as an emergency situations or rescue operation, medical assistance, disaster relief services, mine site operations, and military mobile network in battlefields. In MANETs, identification of malicious node is very hard because mobile node has volatile nature.

Fig 1: Mobile Ad Hoc Network [11]

Security is providing protected communication between mobile nodes in wireless network. Many routing protocols are available for MANET. It has been proposed to facilitate rapid and efficient network design and restructuring.

2. AODV ROUTING PROTOCOL

Ad hoc on-demand distance vector (AODV) is a reactive routing protocol which is designed for ad hoc network. Route is not predefine it established when it's needed. AODV routing protocol is used for both unicast routing as well as multicast routing. AODV uses a sequence number for find the routing message is fresh. It applies a destination sequence numbers for finding the fresher path. AODV has three types of controlling message RREQ, RREP, RERR.

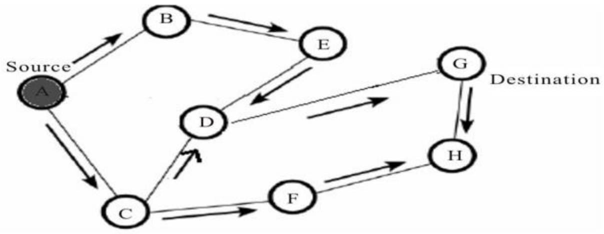

Fig 2: RREQ Broadcast

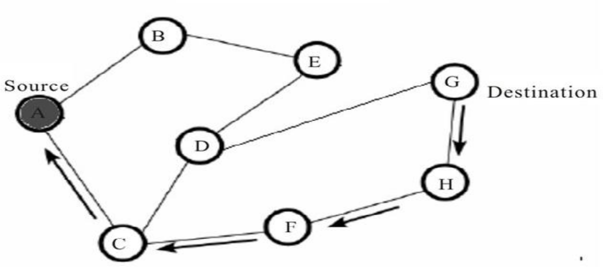

Fig 3: RREP Forwarded Path

In an AODV, RREQ is used for the route broadcasting. Source node uses this route request packet for broadcast the route request. RREP is route reply which is send if node has a valid route to the destination.

3. WORM HOLE ATTACK

Among various attacks, worm hole is very dangerous as it does not exploit any other node in the network. Due to wormhole attack on proactive type of protocol like AODV first it generates the tunnel between two malicious nodes. In this tunnel it contains data packet for a long time so in result End –to –End delay is affected. In both proactive and reactive routing protocol wormhole attack has significant impact. It performs an operation like packet dropping while it shows in low network throughput.

Tunnel is being generated by using out band or in band channel. Tunnel tried to show direct path between source and destination. This make the tunnelled packet get there either faster or with minimum hops compared to the simple multi hop path on which packet will be transmitted. This creates a false impression crated by this comparison that the two end points of the tunnel also say wormhole points are very close to each other means that that one is a shorter route.

In the following figure s2 and s9 are two malicious end nodes that makes wormhole tunnel to received RREQ packets.

Malicious node s9 send a packet with a fake route which is s9 to s2, which is not an actual path. Actual path is s9-s8-s6-s5-s4-s2. Route s9 to s2 creates false impression.

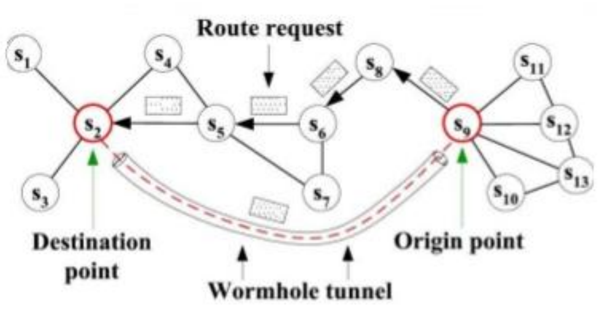

Fig 4: Wormhole attack [9]

4. RELATED WORK

The various techniques used for the prevention and detection of wormhole attack in MANET is described below:

4.1 Packet Leashes

In this paper [6], the method is used to detect wormhole attack, Temporal Leashes and Geographical Leashes. Temporal Leashes is used a sending and receiving mechanism. Geographical Leashes is based on location of nodes.

1. **Temporal Leashes:** All modes must need strongly synchronized clock. It is based on off- the -shelf hardware.
2. **Geographical Leashes***:* There is no requirement of clock synchronization. It requires GPS hardware.

4.2 Directional Antennas

It is a hardware based approach [7] in which each node are used directional antennas for communication purpose. Use specific sectors of antennas and observe the direction of received signal. This technique fails if an attacker intentionally places the wormhole between the communicating nodes.

4.2 Digital Signature

This paper [8] is presented a method which is useful to prevent a wormhole attack in the network. In this method each node contain digital signature of every nodes of a network. Verify a digital signature of sender nodes by receiver node. Using this verification it create trusted path between sender and receiver. If malicious node present it is identify because that node does not have true digital signature.

4.3 Neighbor Node Analysis

In this paper [10] neighbor node approach analyze the entire neighbor node for the purpose of authentication, so that secure transmission can be occur over the wireless network. This method is use request and response mechanism. Node send a request to all neighbor nodes. The node will maintain a table which store a reply time. If reply time is not accurate there is a harmful node in the current network. Comparison is done between the response time of RREP message and the response time of actual message sent. If response time of actual message is greater than the response time of RREP + threshold value than we can say that wormhole link is present in the route. Comparison of this process is repeated till the destination reached.

4.4 DelPHI Technique

Delay Per Hop Indication [9] is based on the calculation of (delay per hop) value of disjoint paths. It is based on the fact that, the delay a packet experiences in propagates one hop should be comparable along each hop path. While in the wormhole attack, delay for propagating across fake neighbours are high as there are many hops between them. It doesn't need any extra hardware or tight time synchronization and has high power efficiency [9]. It works for both In-Band and Out of –Band mode.

4.5 WHOP Technique

This paper [12] proposes WHOP technique in which a node send extra packet which is called hound packet after the route request is send. From source to destination there are many routes available but the hound packet is processed by the packet in which the packets are involved with source to destination. WHOP contains other three column address of node processing bit (PB) and count to reach next hop (CRNH). CRNH represents the hop difference between neighbors of one hop separated node. At each node CRNH value is increment + 1 from the first.

5. PROPOSED SCHEME

We use path tracing algorithm and in our work we use two parameters for finding wormhole link or path: 1) hop count 2) RTT (delay). In our work, we calculate delay/hop count ratio when RREP receive by sender. When sender broadcast RREQ message for particular destination, each intermediate node will increase hop count, add its own id and increase time stamp values and further broadcast RREQ message. Initially each node maintain routing table of particular destination with particular hop count and delay product. Now when receiver get back RREP message, source first compare delay/hop count. This ratio compare with threshold value which previously counted by source. If this ratio is too large then simply discard RREP message.

During wormhole attack, sender broadcast RREQ message, it receive by Attacker node M1 and M1 encapsulate this message with payload and directly send to other Attacker M2 because it create dedicated link between M1 and M2 but here are wormhole attack, propagation in between the wrong neighbor the delay should be irrationally high. Hence, if we compare the delay/hop of a simple path and the wormhole path, we have to show that the simple path delay/hop is minor. If we find the high different value for delay/hop count is leads to a Wormhole Attack.

Behavior of wormhole attacker like less hop count so when it send back RREP message, at that time sender simply don't consider this path as a best route instead it verify consecutive delay and hop count. It calculates delay/hop count ratio with previously calculated for best route. Using this technique we can improve throughput, packet delivery ratio and end2end delay parameters of AODV over MANET.

6. SIMULATION RESULT

6.1 Performance Matrices:

6.1.1 Throughput:

In the specified time amount of data transfer for one point of network to another point and the rate for using transmitted data is known as throughput.

6.1.2 Packet Delivery Ratio:

It is the ratio between total number of received packet to the total number of packet send by source node or sender node over a network.

6.1.3 End to End delay:

A data will requires some time to transmit the data from source to destination node; it is called End-to-end delay.

6.2 Simulation Parameters:

Table 1 : Simulation Parameter

Parameter	Value
Network Simulator	NS2.35
Simulation Time	100 s
No of Mobile Nodes	25,50,75,100
No of Wormhole	1 to 4
Topology	500 m x 500 m
Routing Protocol	AODV
Traffic	CBR
Packet Size	512 Bytes/Packet
Pause Time(t)	2.0 s
Maximum Speed(M)	4.0 m/s
Mobility Model	Random Way Point
MAC Protocol	802.11

6.3 Impact of Number of Node:

6.3.1 Graph for Throughput vs. No of Node:

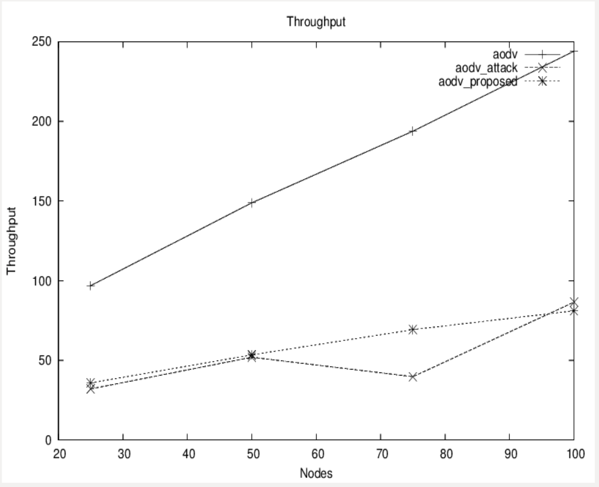

Fig 5: Throughput vs. No of Node

The graph describe that the effect of the no. of nodes on throughput. The first observation is that AODV protocol has a high throughput because of it takes attack free path for packet delivery. The second observation is AODV (with wormhole attack) protocol suffers from attacking behavior and down the throughput. The third observation is that proposed AODV gives improved performance compared to the wormhole attack. The reason for the improvement is that our proposed solution strongly prevents malicious node.

6.3.2 Graph for Packet Delivery Fraction:

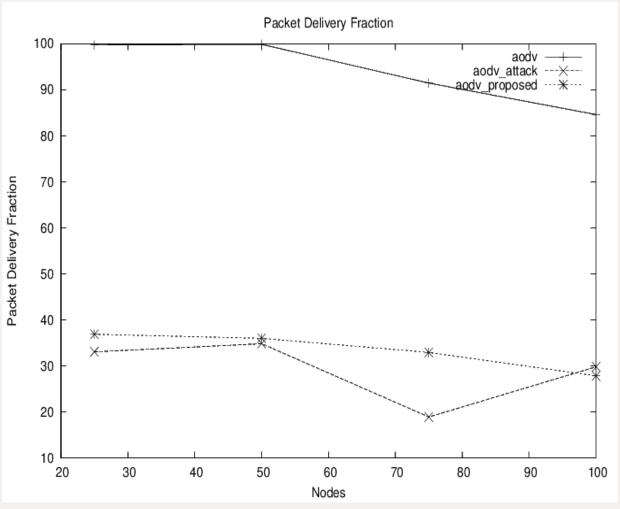

Fig 6: Packet Delivery Fraction

The graph describe that the effect of the no. of nodes on PDF. The first observation is that AODV protocol has a higher PDF compared to remaining both. The second observation is that AODV (with wormhole attack) having very less PDF because it shows its attacking behavior and decrease the performance of PDF. Third observation is that the PDF is higher in our proposed scheme as compared to wormhole attack even though the number of nodes is increasing.

6.3.3 Graph for End to End Delay:

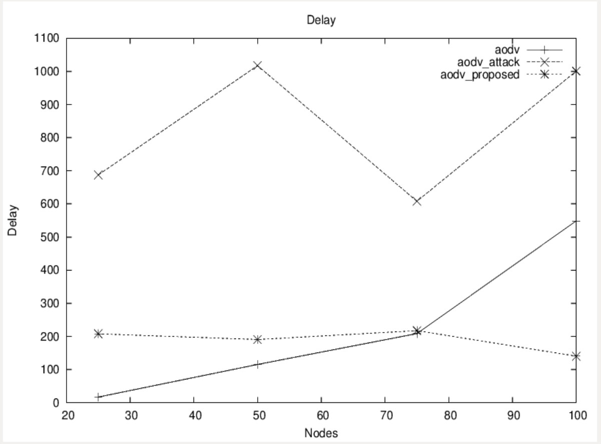

Fig 7: End to End Delay

The graph describe that the effect of the no. of nodes on end-to-end delay. The first observation is that AODV protocol has a less delay compared to AODV (with wormhole attack) protocol because it takes safe n attack free route. The second observation is AODV with worm hole attack has maximum delay compared to the reaming both. The third observation is that our proposed scheme give minimum delay compared to simple AODV protocol because it detect attacker node and eliminate it from the network.

6.4 Impact of number of Malicious Node:

6.4.1 Graph for throughput vs. Number of Malicious Node:

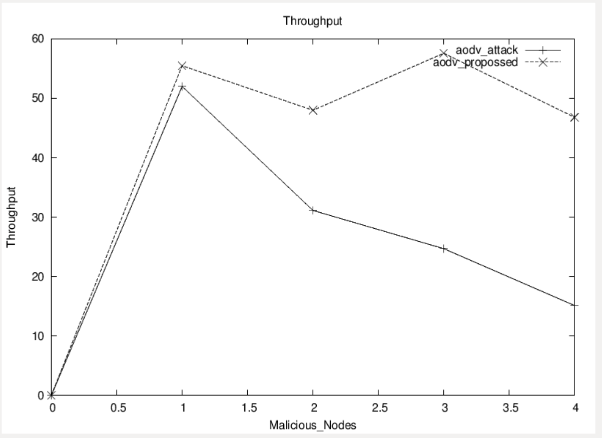

Fig 8: Throughput vs. Malicious nodes

The graph describe that the effect of the malicious nodes on throughput. In AODV (with wormhole attack) protocol and our proposed scheme when no of malicious node increases, throughput is decreases accordingly but compared to AODV (with wormhole attack) protocol throughput increases in our proposed work

6.4.2 Graph for PDF vs. Number of Malicious Node:

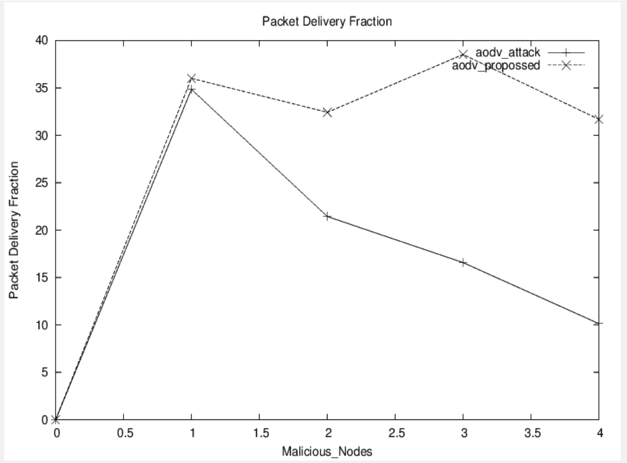

Fig 9: Packet Delivery Fraction vs. Malicious nodes

The graph describe that the effect of the malicious nodes on Packet Delivery fraction. In AODV (with wormhole attack) protocol and our proposed scheme when no of malicious node increases, packet delivery fraction is decreases accordingly but compared to AODV (with wormhole attack) protocol Packet Delivery Fraction increases in our proposed work.

6.4.3 Graph for Delay vs. Number of Malicious Node:

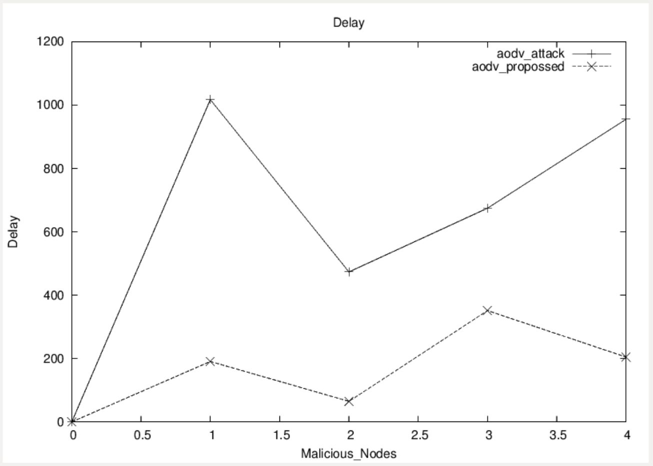

Fig 10: Delay vs. Malicious node

The graph describe that the effect of the malicious nodes on delay. In AODV (with wormhole attack) protocol and our proposed scheme when no of malicious node increases, End to end Delay is not always increase but compared to AODV (with wormhole attack) protocol End to End Delay decreases in our proposed work.

7. CONCLUSIONS

MANET is a wide area in which security is major challenge. Due to absence of centralize controller the network suffers from many security attack.In this paper, we have analysed the different types of attacks and protocols which degrade the performance of the network. Also different techniques are compared to detect and prevent wormhole attack. We have in our proposed work Source first compares delay/hop count. This ratio compare with threshold value which previously counted by source. If this ratio is too large then simply discard RREP message. By using our proposed work parameters like End-to-End delay, Throughput and Packet Delivery Fraction gives us a better performance with compare to AODV with attack. In future we can compare other parameter with and without attack.

8. ACKNOWLEDGMENT

I would like to thank everyone who helped me in my research work. I would like to thank my supervisor Prof. Haresh Rathod I am very happy that you gave me the opportunity to continue my research during last two years.

9. REFERENCES

[1] Robinpreet Kaur and Mritunjay Kumar Rai , “A Novel Review on Routing Protocols in MANETs” , *Undergraduate Academic Research Journal (UARJ)*, Volume-1, Issue-1, 2012.

[2] PRADIP M. JAWANDHIYA and MANGESH M. GHONGE, “A Survey of Mobile Ad Hoc Network Attacks”, *International Journal of Engineering Science and Technology*, Vol. 2(9), pp.- 4063-4071, 2010.

[3] M.H. davda, s.r.javid “A review paper on the study of attacks in MANET with its detection and mitigation scheams ” *IJARCSMS*, april 2014.

[4] C. Siva Ram Murthy and B.S.Manoj, “Ad hoc Wireless Networks” (Chapter 7), 2014.

[5] E.M.Royer and C.E.Perkins, “Adhoc On-Demand Distance Vector Routing”, *IEEE*, pp. 90-100, February 1999.

[6] Yih-Chun Hu, Adrian Perrig, David B. Johnson, “Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks”, *IEEE* 2003.

[7] L. Hu and D. Evans, “Using directional antennas to prevent wormhole attacks”. In the *Proceedings of network & distributed system Security Symposium,*, February 2004.

[8] Pallavi Sharma, Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature”, *IEEE*, 2011.

[9] Lui K.-S., sChiu H.S., “DelPHI: Wormhole Detection mechanism for *Adhoc* Wireless Networks” Proceedings of the 1st International Symposium on Wireless Pervasive Computing; Phuket, Thailand. 16–18 January 2006.

[10] Sweety goyai, harish rohil, “Securing MANET against Wormhole Attacl using Neighbour Node Analysis” *IJCA* volume 81,November 2013

[11] Saleh Ali K.Al-Omari1, Putra Sumari2 “An overview of a mobile ad hoc networks for the existing protocols and application”, International journal of graph theory in wireless Adhoc network, March-2012.

[12] Saurabh Gupta, Subrat Kar, S Dharmaraja, “WHOP: Wormhole Attack Detection Protocol using Hound Packet”, *IEEE*, 2011**.**